IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES FOR: AN ANTICIPATORY SEARCH WARRANT FOR THE RESIDENCE LOCATED AT: 1056 DRAKETOWN ROAD, CONFLUENCE, PA 15424	Magistrate No. 3:21-65 **[UNDER SEAL]**

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A SEARCH AND SEIZURE WARRANT

I, Dan Carney, being duly sworn, do hereby state the following:

I. INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent (SA) with Homeland Security Investigations (HSI) in Pittsburgh, Pennsylvania and have been so employed for approximately ten (10) years. As such, I am an "investigative or law enforcement officer of the United States" within the meaning of 18, U.S.C. § 2501(7). That is; an officer of the United States, who is empowered by law to conduct investigations of, and make arrests for, offenses against the United States.

2. I have successfully completed the Criminal Investigator Training Program (CITP) and the ICE Special Agent Training Program (ICESAT) at the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia and have experience in the investigation and prosecution of violations of immigration, customs (import/export), financial, narcotics, and other federal criminal laws. I am currently assigned to the HSI Pittsburgh office-Group III; encompassing counter proliferation, customs fraud, and document/benefit fraud investigations. I have previously executed and participated in the execution of numerous search warrants.

3. The facts set forth in this Affidavit are based upon my personal observations, my training and experience, and information provided by other law enforcement officers who are also

involved in this investigation, including the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) and the U.S. Postal Inspection Service (USPIS). Because this Affidavit is submitted for the limited purpose of establishing probable cause, I have not set forth each and every fact known to this investigation. Additionally, the incidents described herein occurred a short time ago; the investigation is ongoing and in its preliminary stages.

4. This Affidavit is made in support of an application under Fed. R. Crim. P. 41 for a search and seizure warrant for the premises at 1056 Draketown Road, Confluence, Pennsylvania 15424 (hereafter, **SUBJECT PREMISES**), as described more fully in Attachment A.

5. Your Affiant seeks authorization to search for and seize evidence, instrumentalities, contraband and fruits of violations of 18 U.S.C. § 545 - Smuggling goods into the United States; 18 U.S.C. § 541 - Entry of goods falsely classified; 18 U.S.C. § 922(l) - Unlawful importation of a firearm[1]; 26 U.S.C. § 5861(d) - Possession of unregistered firearms, 26 U.S.C. § 5844 - Unlawful importation of a firearm, and 18 U.S.C. § 922(g)(1) - Possession of a firearm by a convicted felon (collectively, the "**TARGET OFFENSES**"), as described more fully in Attachment B.

6. As discussed below, a shipment of two (2) firearm suppressors, a/k/a "silencer" contained in a China Post international mail parcel originating from China was recently seized by Customs and Border Protection (CBP) officers at the Los Angeles International Mail Facility in Los Angeles, California.

7. This shipment was addressed to "Ted Watrin" at the **SUBJECT PREMISES** and was declared as a "Filter", with a declared value of $10.00 (USD) and a declared weight of 0.3 KG.

---

1. Under the Gun Control Act of 1968 [18 USC § 921(a)(3)] and the National Firearm Act of 1934 [26 USC § 5845(a)], the definition of a firearm includes any firearm muffler or firearm silencer.

8. Your Affiant proposes to attempt a controlled delivery of the above parcel to the **SUBJECT PREMISES**, its intended delivery address.

9. If the parcel is accepted by an occupant of the residence and taken into the **SUBJECT PREMISES**, your Affiant submits there will be probable cause that inside of the residence at the **SUBJECT PREMISES**, there will be evidence of violations of the **TARGET OFFENSES**.

II. BACKGROUND ON NATIONAL FIREARMS ACT (NFA) ITEMS

10. Based upon your Affiant's training, experience, and discussions with other federal agents familiar with National Firearms Act (NFA) violations, your Affiant is aware that firearm suppressors, also known as "silencers," vary by design and appearance, but all, when properly installed, will silence, muffle or diminish, the report of a portable firearm.

11. These items are regulated by both the National Firearms Act of 1934 and the Gun Control Act of 1968.

a. Under 18 U.S.C. § 921(a)(24) the terms "firearm silencer" and "firearm muffler" mean any device for silencing, muffling, or diminishing the report of a portable firearm, including any combination of parts, designed or redesigned, and intended for use in assembling or fabricating a firearm silencer or firearm muffler, and any part intended only for use in such assembly or fabrication.

b. Under 26 U.S.C. 5845(a), a "silencer" is defined as a type of NFA firearm subject to regulation by the Act.

12. The making or importation of a suppressor must be approved in advance by the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF).

13. To make a silencer, an individual must file an ATF Form 1, (Application to Make and Register a Firearm), pay a $200.00 USD tax, and comply with all other provisions of the law prior to making the firearm.

14. Approval of the Form 1 results in the registration of the firearm in the National Firearms Registration and Transfer Record (NFRTR). Any subsequent transfers must be approved in advance by the ATF.

15. To import a silencer into the United States, an individual must file an ATF Form 6 (Application and Permit for Importation of Firearms, Ammunition, and Defense Articles), which must be approved by the ATF prior to the importation.

16. Firearms silencers and suppressors have also been designated as defense articles subject to the controls of the U.S. Munitions Import List (USMIL) under Category I – Firearms, pursuant to section 38(a) of the Arms Export Control Act, 22 U.S.C. 2778(a), and E.O. 13637.

17. Currently, these items may not be imported from China because China is listed as a restricted country under 27 CFR § 447.52(a) as a result of the arms embargo currently in place against that country.

III. BACKGROUND ON ILLICIT FIREARMS TRAFFICKING

18. Based upon my training, experience, and discussions with other federal agents related to the investigation of international import-related National Firearms Act (NFA) violations, I am aware that:

a. With the proper knowledge, computer software, and machining equipment, individuals have the ability to manufacture semi-automatic firearms, fully-automatic machineguns, and firearm suppressors from scratch. These items can be

manufactured with the use of lathes or computer numerical controlled (CNC) milling machines, which are digitally automated machining centers capable of cutting and fabricating solid materials including firearms parts. With this type of equipment, a subject can manufacture firearms that perform as well as those created by licensed manufacturers, and they can place any type of markings, symbols, or serial numbers that the maker desires, or omit such markings.

b. Firearms and ammunition trafficking organizations have developed a number of methods to insulate their illegal activities from detection by law enforcement. These methods are common to major firearms and ammunition trafficking organizations to varying degrees of sophistication.

c. Illegal firearm and ammunition traffickers often utilize techniques to prevent the detection of firearms that are shipped unlawfully through mail and common carriers by means of falsifying invoices, bills of sale, shipping papers, and customs forms by listing the firearms as other items which include, but are not limited to, firearms parts and pieces (rather than firearms) and components utilized in the automotive, industrial, and machinery industries. In addition, illegal firearm traffickers have been known to conceal firearms inside of other objects to avoid detection by law enforcement officials.

d. Individuals involved with illegal firearm and ammunition trafficking activity will often wear latex or vinyl gloves while handling firearms and ammunition while processing packages for shipment. This is done in order to prevent fingerprints from being left on items that could later be used as evidence against them.

e. Individuals involved with illegal firearm and ammunition trafficking activity often use complex methods for ordering, paying for, and transferring the firearms, firearm components, and/or ammunition. These traffickers utilize payment methods that are often difficult to trace, which include: U.S. currency, money orders, wire-transfers, PayPal transactions and pre-paid credit cards. These traffickers utilize these methods in order to minimize the ability of law enforcement officials to identify the original source of funds.

f. Persons engaged in illegal firearm and ammunition trafficking activity typically maintain at their residences, places of business, storage lockers, in their vehicles and other locations under their control, items constituting fruits, instrumentalities, and evidence of their criminal activities and associations. These items can include firearms (used to protect the above items and profits), packaging materials, financial records, personal address/telephone books identifying co-conspirators, large sums of U.S. currency in excess of $1,000 not immediately traceable to legitimate activity, indicia of control/ownership, and other items more particularly described in Attachment B and incorporated herein by reference.

g. Illegal firearm and ammunition trafficking activity often earns substantial cash proceeds that traffickers accumulate or convert to other assets, such as jewelry, vehicles, real estate, bank accounts, or other investments. Financial and business records are often kept for firearm and ammunition trafficking activity and/or the accumulation/transformation of illicit proceeds.

h. Individuals involved in illegal firearm and ammunition trafficking activity will often conceal illicit firearms, illicit firearm parts, proceeds, documents, and other

facilitating property in vehicles, garages, or other buildings at a location under their control. Such vehicles are often registered in the name of other individuals.

i. Individuals involved in illegal firearm and ammunition trafficking activity often store illicit items, proceeds, and other illicit firearms brokering relating property offsite in storage units and safe deposit boxes. Such individuals often keep records of such locations and or the keys to them at their residences or other places under their control.

j. Individuals involved in illegal firearm and ammunition trafficking activity often use digital devices such as cell phones, computers, and tablets in furtherance of their illicit distribution activities. Such devices are used to communicate with suppliers and customers, and a host of other activities.

IV. BACKGROUND INFORMATION CONCERNING Theodore WATRIN

19. According to the Accurint consumer database, Theodore WATRIN is associated with the **SUBJECT PREMISES**.

20. A query of the Pennsylvania Department of Transportation (PennDOT) driver license database indicates that the Commonwealth of Pennsylvania issued a driver's license (OLN: 30 853 628) to Theodore WATRIN (DOB: 06/03/1968), but that it is suspended due to DUIs. The address of record listed on the associated PennDOT "Details" record is the **SUBJECT PREMISES**.

21. A query of PennDOT vehicle registration records by the Pennsylvania Criminal Intelligence Center (PaCIC) indicates that WATRIN has no vehicles registered to him in the Commonwealth of Pennsylvania.

22. A criminal history query of WATRIN in the Interstate Identification Index (III) revealed a criminal arrest by the Albuquerque, New Mexico Police Department on February 22, 1991

under FBI#: 970790KA1 for violation of Trafficking by Distribution, New Mexico Statute 30-31-20(A)(2). WATRIN pled guilty and was subsequently sentenced to three years of probation (case # D-202-CR-199100814).

23. Additional queries reveals that WATRIN has not been issued a Pennsylvania License to Carry Firearms and the Pennsylvania Record of Sale database had no records of handgun purchases by him.

24. A query by the ATF of the Federal Licensing System (FLS) reveals that WATRIN has not been granted a federal firearms license (FFL) to engage in business as a firearms dealer. Also, he does not have any record of any NFA items registered to him in the National Firearm Registration and Transfer Record. Also, a search for any ATF Form 6 applications filed by WATRIN was conducted by the ATF with negative results.

V. BACKGROUND INFORMATION CONCERNING Susan Sabatula

25. According to the Accurint consumer database, Susan Sabatula is associated with the **SUBJECT PREMISES**.

26. A query of the Somerset County website which contains property records, indicates the **SUBJECT PREMISES** is owned by Susan Sabatula.

27. A query of the Pennsylvania Department of Transportation (PennDOT) driver license database indicates that the Commonwealth of Pennsylvania issued a driver's license (OLN: 17 115 751) to Susan Sabatula (DOB: 10/21/1957) on August 14, 2018, which expires on October 22, 2022. The listed driver's address is the **SUBJECT PREMISES**.

28. Additional queries reveal that Sabatula has not been issued a Pennsylvania License to Carry Firearms and the Pennsylvania Record of Sale database had no records of handgun purchases by her.

29. On April 8, 2021, Your Affiant and HSI Pittsburgh Special Agent Michael Pausic performed a "drive-by surveillance" of the **SUBJECT PREMISES** [2] and took photographs of the property. As described more fully in Attachment A, the property is a two-story brown house, with a brown roof, residential dwelling. There is also a two-car detached garage with white siding on the front of the unit.

VI. PROBABLE CAUSE

30. On April 8, 2021, CBP Officer M. Pena seized a shipment containing two (2) firearm suppressor, a/k/a "silencer," (referred to as the **SUBJECT PARCEL)** during examination of international mail parcels from China at Los Angeles International Mail Facility near Los Angeles, California.

31. The **SUBJECT PARCEL** bore U.S. Postal Service (USPS) Tracking Number LY697420591CN and was addressed to Ted WATRIN at the **SUBJECT PREMISES**.

32. CBP seized this item as a prohibited importation under FP&F# 2021272000216301, for violation of Title 19, United States Code, Section 1595a(c)(1)(C) and Title 49, United States Code, Section 80302(a)(2) and forwarded the item to HSI Pittsburgh for further investigation.

33. On April 12, 2021, SA Carney examined and photographed the package and its contents at the HSI Pittsburgh office and noted the following:

a. The mailing label and customs declaration listed the addressee as:

Ship To: Ted Watrin
1056 Draketown Road
Confluence Pennsylvania 15424
USAPHONE: / 000000

b. The mailing label and customs declaration listed a return address of:

From: XU SHI MING
YONGFENGXIANG DALUOJIAZUI
CUN 206 HAO HANYANG Wuhan
Hubei 430000
China

c. On the customs declaration, the contents of the parcel were manifested as:

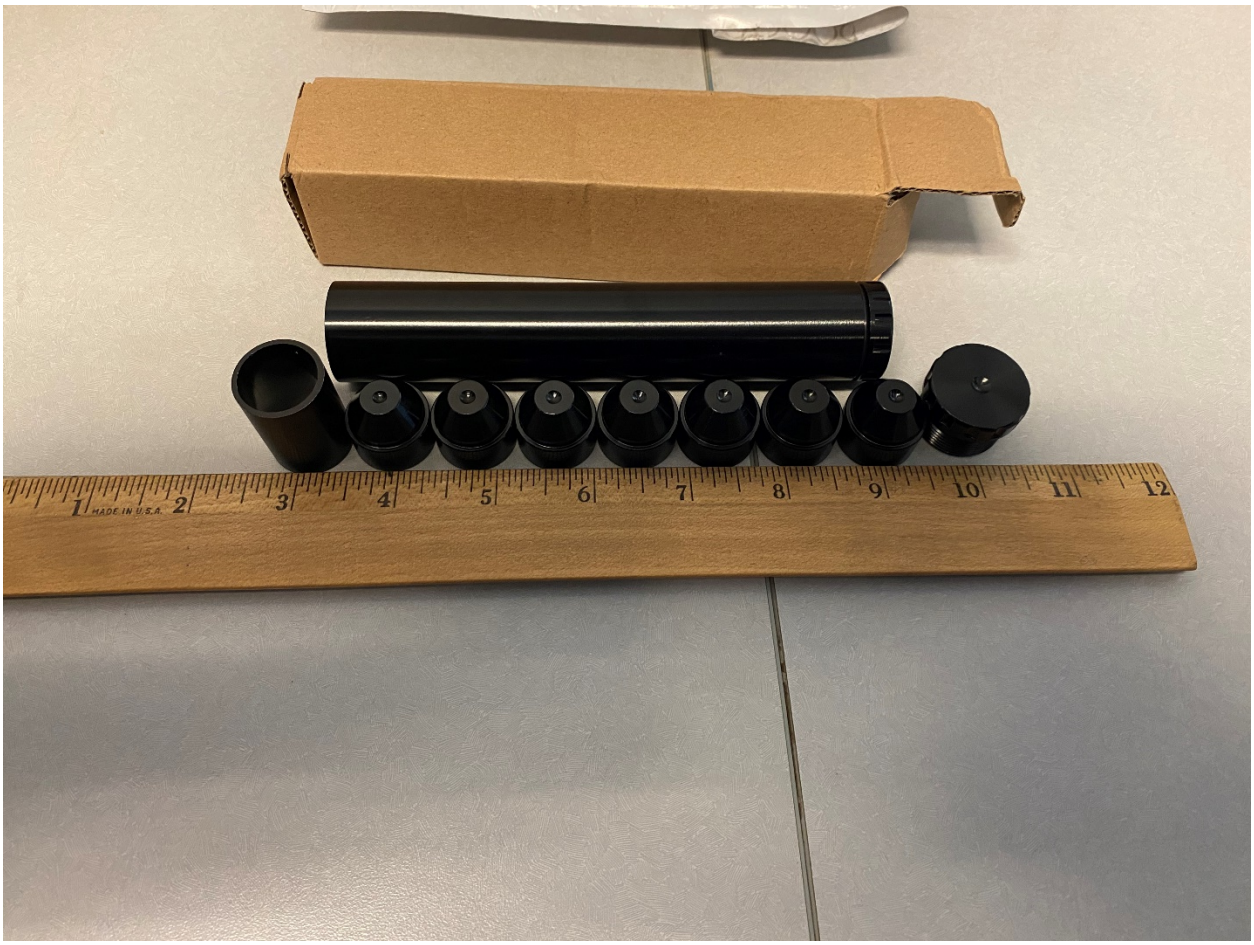
Description of Contents	Total Kg	Val(US$)
Filter x 2	0.3	10.00

d. Following "Sender's signature& Data Signed:" (sic) was the date 2021-03-10.

34. Your Affiant physically inspected the contents of the above parcel, which contained two small cardboard boxes. On the outside of the boxes were a white label bearing the numerals "1/2-28" along with what appear to be Chinese characters. Firearm silencers come in standard thread patterns (also known as "thread pitches) to enable them to be attached to the barrel of a firearm having corresponding threads. "1/2-28" is one of several common thread pitches used by firearms manufacturers.

35. The parcel also contained (2) metal cylinder tube, black in color. The cylinder tube bears no visible manufacturer's markings or serial number. A black threaded metal cap was screwed on one (1) end of the tube. A black solid metal cap was screwed on the other end of the cylinder tube. When the end caps were removed, seven (7) metal baffles and one (1) metal spacer, all black in color, could be removed from the metal cylinder tube.


CN22
MADE IN U.S.A.



36. There has been a recent, drastic, increase in the number of firearm suppressors being illicitly introduced into the commerce of the United States via Airmail from China.

37. CBP has encountered these suppressors in large numbers at various international mail facilities around the United States. CBP has partnered with HSI and ATF to combat the flow of these contraband items into the United States.

38. The intercepted packages have been falsely manifested, incorrectly identifying the contents of the packages as "filters," "machine filter nozzle," "motorcycle filter," and other terms with the similar terms in the commodity description.

39. Although a definitive classification would have to be made by a qualified laboratory, such as the ATF's Firearms and Technology Criminal Branch, your Affiant believes based on his

training, experience, and available reference information that there is probable cause the recovered device is a "firearm silencer" and a "firearm" as defined under Title 18, United States Code, Section 921(a)(24), 921(a)(3) and Title 26, United States Code, Section 5485(a).

VII. ELECTRONIC EVIDENCE, DIGITAL DEVICES[3], AND FORENSIC ANALYSIS

40. As described above and in Attachment B, this application seeks permission to search for records that might be found on the **SUBJECT PREMISES**, in whatever form they are found.

41. One (1) form in which the records might be found is data stored on a computer's hard drive or other storage media (including cellular telephones). Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

42. In my experience, individuals conduct a considerable amount of communication using their cellular telephone, and those communications are in the form of voice calls, text messages, SMS messages, MMS messages, e-mails, social media messages and posts, and messages shared via "chat" applications.

43. Individuals who conspire with one another to conduct illegal activities do so through the use of cell phones and other electronic devices to communicate through social media and/or contact one another by the use of phones to speak directly to or send text messages. There is probable

---

2. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as paging devices, mobile telephones, and smart phones; digital cameras; gaming consoles; peripheral input/output devices, such as keyboards, printers, scanners, monitors, and drives; related communications devices, such as modems, routers, cables, and connections; storage media; and security devices.

cause to believe that WATRIN and others (including parts suppliers and other firearms suppressor purchasers) would have communicated through such methods regarding the unlawful purchase of firearms and subsequent unlawful transfers of the firearm(s). I also know that individuals often utilize their cellular phone and smartphones to access the Internet. I also know that each time a device is used to access the Internet, the device maintains a record or "browser history," showing which websites were visited and when. Based upon your Affiant's training and experience, I believe that WATRIN was likely to access the internet for information about firearms, firearm parts, to include types of firearms, prices, and the locations of dealers.

44. I also know through training and experience, as well as through consultation with a trained cellular phone forensic examiner, that evidence of the above forms of communication and the browser history are often kept in cell phones for months and even years at a time. I am also aware that a forensic examiner may be able to recover messages and other data that were manually deleted by the user of the phone. For these reasons, I believe that cellular phones and smartphones utilized by WATRIN. will contain communications from the time the firearm suppressor was intercepted by CBP was purchased. For all of these reasons, I request authorization to seize and search any cellular phones or smartphones found in the **SUBJECT PREMISES**.

45. *Probable cause.* I submit that if a computer, cellular device, or storage medium is found in the **SUBJECT PREMISES**, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Because this investigation involved the purchase and the unlawful importation of a firearm suppressor exported from China, there is reason to believe that a computer or cellular device was used for that purchase and there may be a computer system or cellular device located in the **SUBJECT PREMISES**. These

devices have been found listed for sale online through shopping applications such as "Wish." Usage of the "Wish" application requires a user to utilize a computer or cellular device in order to place and execute transaction and track the future delivery of the purchase to the intended address.

b. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

c. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

d. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation; file system data structures, and virtual memory "swap" or paging files. Computer users

typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

e. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

46. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the **SUBJECT PREMISES** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical

location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data

stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain prohibited items, it is an instrumentality and also a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

47. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a location for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the location, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of

the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on the location could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the location. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

48. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

VIII. CONCLUSION

49. On or about April 20, 2021, your Affiant along with additional law enforcement personnel will attempt a controlled delivery of the **SUBJECT PARCEL** to the **SUBJECT PREMISES**.

50. Based on the foregoing, upon the **SUBJECT PARCEL** being taken into the **SUBJECT PREMISES**, I submit that there will be probable cause to believe that at the **SUBJECT PREMISES** more fully described in Attachment A, evidence of violations of 18 U.S.C. § 545, Smuggling goods into the United States; 18 U.S.C. § 541, Entry of goods falsely classified; 18 U.S.C. § 922(l), Unlawful importation of a firearm; 26 U.S.C. § 5861(d), Possession of unregistered firearms; 26 U.S.C. § 5844, Unlawful importation of a firearm; and 18 U.S.C. § 922(g)(1), Possession of a firearm by a convicted felon, will be found therein.

51. The triggering event for the execution of the anticipatory search warrant will be the SUBJECT PARCEL being accepted and taken into the SUBJECT PREMISES.

52. If the triggering event does not occur, the search warrant will not be executed.

53. If the triggering event does occur, your Affiant believes within the residence located at the **SUBJECT PREMISES** will be the items described in Attachment B.

54. Your Affiant therefore respectfully requests that this Court issue a warrant authorizing the search of the location set forth in the Affidavit and attachments and authorizing seizure of the items more specifically described in Attachment B.

55. Because this investigation is ongoing, it is further respectfully requested that this Application and any warrant or orders issued thereon be ordered sealed until further notice.

Respectfully submitted,

/s/ Dan Carney
Dan Carney
Special Agent
Homeland Security Investigations

Sworn and subscribed before me, by telephone
pursuant to Fed. R. Crim. P. 4.1(b)(2)(A),
this 13th day of April, 2021.

_____
Keith A. Pesto
United States Magistrate Judge